Влияние цифровой трансформации банковского сектора на профиль операционного риска кредитных организаций

Яковлев Никифор Алексеевич
аспирант, кафедра экономики и общего менеджмента, Московский институт экономики, политики и права (МИЭПП), yakovlev.nikifor@mail.ru

Цель исследования состоит в выявлении направлений изменения профиля операционного риска кредитных организаций под влиянием цифровой трансформации и разработке инструмента их сравнительной оценки. Методическую основу составили сравнительный и структурно-логический анализ, концептуальное параметрическое моделирование и однофакторный анализ чувствительности. Информационная база включает документы Банка России и Базельского комитета по банковскому надзору за 2021–2026 гг., а также результаты российских и зарубежных исследований. Установлено, что цифровизация сокращает частоту рутинных ошибок, но может повышать концентрацию, скорость распространения и потенциальную тяжесть технологических, модельных, кибернетических и провайдерских событий. Предложена авторская матрица трансформации профиля операционного риска, связывающая технологии, риск-снижающие эффекты, каналы усиления риска и опережающие индикаторы. Разработана концептуальная скоринговая модель, разделяющая валовой технологический эффект и остаточный риск с учетом зрелости контрольной среды; выведен порог зрелости. Анализ чувствительности при раздельном изменении параметров усиления и снижения риска на ±20% подтвердил устойчивость качественных выводов для примеров ИИ и облачной платформы и выявил пограничность открытых API. Подход может применяться при предварительной оценке цифровых проектов, настройке ключевых индикаторов риска и актуализации системы управления операционным риском.

Ключевые слова: цифровая трансформация, банковский сектор, кредитная организация, операционный риск, профиль риска, искусственный интеллект, облачные технологии, риск третьих сторон, ключевые индикаторы риска.

Введение. Цифровая трансформация банковского сектора охватывает автоматизацию операций, использование искусственного интеллекта и больших данных, развитие открытых программных интерфейсов (API), облачных сервисов, удаленной идентификации и платформенных моделей. В Основных направлениях развития финансовых технологий на период 2025–2027 годов эти решения рассматриваются как средства повышения доступности и качества финансовых услуг, развития конкуренции и снижения издержек [1]. Базельский комитет также отмечает рост эффективности, прозрачности и качества клиентского обслуживания, одновременно указывая на возможность возникновения или усиления операционных уязвимостей [2].

Для системы управления рисками важен не сам факт внедрения цифровой технологии, а изменение сочетания источников, частоты, тяжести и взаимозависимости операционных событий. Автоматизация может устранить повторяющиеся ошибки ручной обработки, но ошибка алгоритма способна одномоментно затронуть большой массив операций. Облачная инфраструктура повышает масштабируемость и резервируемость, однако переносит часть критических зависимостей к внешнему провайдеру. Открытые интерфейсы ускоряют обмен данными, но расширяют поверхность атаки и количество точек отказа. Поэтому линейная оценка цифровизации как фактора только роста либо только снижения операционного риска не отражает фактического механизма его трансформации [2; 8; 11; 16; 17; 21].

В российском регулировании риск информационных систем и риск информационной безопасности включены в состав операционного риска, а модельный риск учитывается применительно к используемым кредитной организацией моделям [3]. Р.Г. Нафиков рассматривает цифровизацию банковской системы через сочетание новых возможностей и рисков управления финансовыми активами [4]. О.В. Савчина и Г.В.К. Медина связывают цифровую трансформацию с изменением банковских продуктов, каналов взаимодействия и конкурентной среды [5]. И.А. Лебедева показывает, что положительные эффекты для банков и клиентов сопровождаются технологическими, информационными и социальными ограничениями [6].

В зарубежной литературе A.W.A. Boot, P. Hoffmann, L. Laeven и L. Ratnovski показывают, как финтех меняет структуру финансового посредничества и источники риска [7]. M.H. Uddin и соавторы выявляют статистически значимую связь цифровой трансформации с операционной риск-экспозицией банков [8]. M. Hu и соавторы анализируют разнонаправленное влияние технологических инноваций на операционный риск [17], а M. He, G. Song и Q. Chen указывают на роль качества внутреннего контроля в связи между финтехом и принятием риска банками [18]. Стадийность цифровой трансформации и необходимость сопоставлять ее с бизнес-метриками раскрыты A. Papathomas и G. Konteos [19]. Исследования M.H. Uddin, S. Mollah и M.H. Ali, а также Z. Chen и соавторов дополняют этот вывод применительно к расходам на кибертехнологии, устойчивости и совокупному риску банков [20; 21].

Несмотря на накопленные результаты, в исследованиях чаще приводятся перечни преимуществ и рисков отдельных технологий. Недостаточно формализована связь между интенсивностью применения технологии, ее разнонаправленным воздействием и зрелостью контрольной среды. Это затрудняет сопоставление цифровых проектов и включение их последствий в действующий профиль операционного риска банка [8; 17–19; 21].

Цель статьи заключается в выявлении закономерностей изменения профиля операционного риска кредитных организаций под влиянием цифровой трансформации и разработке инструмента сравнительной оценки этих изменений. Для достижения цели решаются следующие задачи: разграничить риск-снижающие и риск-усиливающие эффекты ключевых технологий; систематизировать каналы трансформации риска; предложить скоринговую модель остаточного эффекта с учетом зрелости контроля; определить набор опережающих индикаторов для практического мониторинга.

Материалы и методы исследования

Информационную базу исследования составили нормативные и аналитические документы Банка России, публикации Базельского комитета по банковскому надзору и научные статьи, посвященные цифровизации и операционному риску. Временной акцент сделан на источниках 2021–2026 гг., поскольку в этот период были обновлены международные принципы управления операционным риском, опубликованы документы по цифровизации, риску третьих сторон, информационно-коммуникационным технологиям и применению искусственного интеллекта [1–3; 10–16]. Научная часть обзора охватывает российские и зарубежные исследования цифровой трансформации, операционного и банковского риска [4–9; 17–21].

Использованы методы сравнительного анализа, классификации, причинно-следственного и параметрического моделирования, а также однофакторного анализа чувствительности. Единицей анализа выступает связка «цифровая технология — компонент риска — контрольная среда». Сначала для каждой технологии выделяется валовой риск-снижающий эффект, затем

канал возможного усиления риска и, наконец, факторы, определяющие остаточный результат после применения контролей.

Под профилем операционного риска в статье понимается упорядоченная характеристика значимости его компонентов с учетом вероятности, тяжести, скорости реализации и взаимозависимости событий. Для управленческого анализа выделены шесть компонентов: риски персонала и процессов; технологической доступности и изменений; информационной безопасности; моделей и данных; третьих сторон и концентрации; внешнего мошенничества и соблюдения обязательных требований. Такая группировка не заменяет классификацию, установленную Положением Банка России № 716-П, а служит аналитической надстройкой для оценки цифровых проектов [3; 14; 16].

Подход имеет концептуально-методический характер. Он не претендует на расчет регуляторного капитала и не использует условные оценки как фактические данные конкретного банка. Источниками калибровки при практическом применении должны быть внутренняя база событий и потерь, ключевые индикаторы риска, результаты аудита, сценарного анализа, тестирования непрерывности и оценки поставщиков. Эти источники соответствуют регуляторной логике управления операционным риском и операционной устойчивостью [3; 10; 11; 14; 16].

Результаты и обсуждение

Сопоставление источников позволяет выделить четыре устойчивых направления изменения операционного риска. Во-первых, уменьшается частота изолированных ошибок при выполнении стандартизируемых операций. Автоматические проверки, сквозная обработка данных и контроль обязательных полей сокращают зависимость от ручного ввода и индивидуального соблюдения процедуры [2; 4–6; 17; 19].

Во-вторых, возрастает масштаб единичной ошибки. Если неверное правило встроено в алгоритм, модель или централизованную платформу, одно отклонение тиражируется на значительное число операций. Скорость цифрового обслуживания уменьшает время между возникновением дефекта и накоплением последствий, поэтому традиционный контроль по итогам отчетного периода может сработать с опозданием [2; 8; 10; 17; 21].

В-третьих, усиливается взаимозависимость компонентов. API, облачные сервисы и внешние программные решения формируют цепочки поставки, в которых отказ или компрометация одного узла затрагивает несколько процессов. Базельский комитет связывает цифровизацию с ростом зависимости от поставщиков и их субподрядчиков, а также с концентрацией услуг у ограниченного круга провайдеров [11]. Обзор Банка России за 2025 год фиксирует увеличение атак на менее защищенную инфраструктуру поставщиков и сервисных компаний, через которые угроза может передаваться финансовой организации [12]. Управление этими зависимостями составляет часть операционной устойчивости банка [16].

В-четвертых, меняется наблюдаемость риска. Цифровые системы создают более полный массив журналов событий и позволяют выявлять аномалии в реальном времени. Одновременно сложность моделей, недостаточная прослеживаемость данных и ограниченная интерпретируемость решений могут затруднить установление причины ошибки. Для искусственного интеллекта существенны качество данных, дрейф модели, ложные решения, возможность манипулирования входными данными и сохранение работоспособности при инциденте. Эти направления отражены в документах Банка России по развитию финансовых технологий и этике применения искусственного интеллекта, а также в международных материалах по ИКТ-риску [1; 2; 10; 13]. Эмпирические исследования дополнительно указывают на значение технологической архитектуры и качества внутреннего контроля [17; 18].

Указанные изменения показывают: цифровая трансформация прежде всего перераспределяет риск. Профиль смещается от большого числа локальных и сравнительно малых отклонений к меньшему числу потенциально коррелированных событий, способных быстро охватить критический процесс. Итоговое направление сдвига зависит от архитектуры решения, масштаба его использования и зрелости контролей [8; 9; 17; 21].



Рисунок 1 – Механизм трансформации профиля операционного риска

Таблица 1

Матрица трансформации профиля операционного риска

Технология	Риск-снижающий эффект	Канал усиления риска	Опережающие индикаторы
Роботизация и сквозная автоматизация	Снижение ручного ввода, единообразное выполнение правил, полная фиксация действий	Тиражирование ошибки правила; отказ централизованного процесса; дефект при изменении	Доля исключений; ошибки после релиза; число ручных обходов; время восстановления
Искусственный интеллект и машинное обучение	Выявление аномалий и мошенничества; ускорение решений; раннее распознавание отклонений	Дрейф и непрозрачность модели; смещение данных; ошибочная автоматизация; атаки на модель	Дрейф признаков; доля отмен решений; доля ложноположительных и ложноотрицательных решений; просрочка валидации
Открытые API и платформенные интеграции	Сокращение повторного ввода; актуальность данных; стандартизация взаимодействия	Рост поверхности атаки; ошибки аутентификации; каскадный отказ; зависимость от контрагентов	Доля неуспешных запросов; задержка API; инциденты доступа; число критических связей
Облачные сервисы и ИТ-аутсорсинг	Масштабируемость; резервирование; профессиональная поддержка; ускорение обновлений	Концентрация у провайдера; ограниченный контроль; риск субподрядчиков; сложность выхода	Доля критичных сервисов у одного поставщика; RTO (целевое время восстановления) / RPO (допустимая потеря данных); результаты тестов выхода
Большие данные и централизованные платформы	Единое представление данных; автоматические проверки; повышение качества аналитики	Единая точка отказа; нарушение качества или происхождения данных; масштабная утечка	Полнота и точность данных; нарушения прослеживаемости данных (data lineage); число критических наборов без владельца
Удаленные каналы и биометрия	Непрерывность обслуживания; снижение бумажных операций; усиление идентификации	Компрометация учетных данных; синтетические подделки (deepfake); ошибки распознавания; цифровое мошенничество	Ложный допуск / ложный отказ (FAR/FRR); аномальные сессии; доля спорных операций; доступность канала

Источник: составлено автором на основе [2; 8–13; 16–21].

Матрица показывает, что одна и та же технология одновременно воздействует на несколько компонентов риска. Например, искусственный интеллект может снизить риск внешнего мошенничества и увеличить модельный риск; облачный сервис может повысить технологическую устойчивость отдельного банка и усилить концентрационную зависимость на уровне рынка. Поэтому оценка только ожидаемого экономического эффекта либо только перечня угроз приводит к неполному решению [2; 11; 13; 17; 18].

Для формализации предложена концептуальная скоринговая модель. Пусть P_i^0 — исходная оценка i-й компоненты профиля по шкале от 0 до 5, где большее значение соответствует более высокому риску. Для каждой технологии j задаются: w_j — интенсивность и критичность применения технологии (0–1); a_{ij} — сила канала усиления риска (0–2); r_{ij} — сила риск-снижающего эффекта (0–2); m_{ij} — зрелость контрольной среды (0–1). Сначала определяется частный технологический эффект E_{ij}, после чего рассчитывается относительное изменение компоненты:

Используемые шкалы являются безразмерными и задают относительные, а не наблюдаемые физические величины. Коэффициенты m_{ij} и w_j нормированы на интервал 0–1, поскольку отражают соответственно степень зрелости контроля и относительную интенсивность (критичность) применения технологии. Для a_{ij} и r_{ij} используется единая шкала 0–2: 0 соответствует отсутствию соответствующего эффекта, 1 — базовому уровню воздействия, 2 — повышенному относительно базового уровню. Общая шкала для a и r сохраняет симметрию двух каналов; при их совместном пропорциональном пересчете порог m* не меняется, поскольку зависит только от отношения a и r. Линейная форма $a(1 - m)$ и rm выбрана как аппроксимация первого порядка: при $m = 0$ канал усиления реализуется полностью, а риск-снижающий эффект не реализуется; при $m = 1$ — наоборот. Такая спецификация обеспечивает прозрачную интерпретацию в условиях отсутствия данных для надежной оценки выпуклой или вогнутой зависимости. При практической калибровке форма зависимости и границы шкал подлежат эмпирической проверке.

$$E_{ij} = a_{ij}(1 - m_{ij}) - r_{ij}m_{ij}.$$

$$\Delta P_i = \Sigma_j w_j E_{ij} / \Sigma_j w_j,$$

$$P_i^{DT} = \max\{0; \min[5; P_i^0 + \Delta P_i]\}.$$

При отсутствии применяемых технологий значение ΔP_i принимается равным нулю. Положительное ΔP_i означает ухудшение компоненты профиля, отрицательное — ее улучшение. Модель разделяет валовой потенциал технологии и остаточный результат: при низкой зрелости контрольной среды преобладает канал усиления, а при высокой зрелости подавляется источник нового риска и реализуется риск-снижающий эффект. Значимость внутреннего контроля и стадий цифровой зрелости подтверждается

результатами M. He, G. Song и Q. Chen, а также A. Papathomas и G. Konteos [18; 19].

Для отдельной пары «технология — компонент риска» условие нейтрального воздействия получается из равенства $a_{ij}(1 - m_{ij}) = r_{ij}m_{ij}$. Порог зрелости равен:

$m_{ij}^* = a_{ij} / (a_{ij} + r_{ij})$.

Если фактическая зрелость m_{ij} выше порога m_{ij}^*, технология улучшает соответствующую компоненту профиля; если ниже, ее внедрение увеличивает остаточный риск. Порог не является универсальной нормативной величиной. Он показывает, какие требования к контролю должны быть выполнены до масштабирования решения. Чем сильнее потенциальный канал усиления относительно риск-снижающего эффекта, тем более зрелая контрольная среда необходима. Такая интерпретация согласуется с принципами управления операционным риском и операционной устойчивостью [14; 16].

Таблица 2

Демонстрационный расчет остаточного эффекта цифровых проектов (условные значения)

Технология / компонента риска	a	r	m	m*	w_jE_{ij}
ИИ в принятии решений / модели и данные	1,6	1,0	0,40	0,62	+0,448
Облачная платформа / третьи стороны	1,4	1,0	0,70	0,58	−0,252
Открытые API / информационная безопасность	1,2	0,8	0,55	0,60	+0,070

Примечание: a — сила усиления риска; r — риск-снижающий эффект; m — зрелость контроля; m* — порог зрелости; E — частный технологический эффект; w: ИИ — 0,8, облако — 0,9, API — 0,7.

В таблице 2 приведен демонстрационный расчет для трех условных проектов. Значения не относятся к конкретной кредитной организации и показывают только порядок применения модели. Для ИИ-проекта зрелость контроля ниже порога, поэтому вклад в модельный риск положителен. Для облачной платформы зрелость выше порога и риск-снижающий эффект преобладает. По открытым API фактическое значение близко к пороговому, что указывает на необходимость дополнительных контролей до расширения масштаба интеграций.

Для проверки устойчивости порога проведен однофакторный анализ чувствительности: параметры a и r поочередно изменялись на ±20% при неизменности остальных параметров. Для ИИ-проекта диапазон m* составил 0,561–0,667 при фактическом m = 0,40, а для облачной платформы — 0,528–0,636 при m = 0,70; следовательно, знак остаточного эффекта в обоих случаях устойчив. Для открытых API диапазон m* составил 0,545–0,652 при m = 0,55, то есть граница проходит через область фактической оценки и знак эффекта может измениться при умеренной вариации параметров. Тем самым анализ чувствительности подтверждает вывод о пограничном характере API-примера и необходимости его дополнительной калибровки. Коэффициент w на величину m* не влияет и изменяет только масштаб остаточного эффекта.

Практическое применение модели включает пять последовательных действий. Сначала определяется перечень критичных цифровых технологий и процессов, которые от них зависят. Затем для каждой пары технологии и компоненты риска оцениваются a_{ij} и r_{ij}, после чего на основании аудита, тестирования и фактических индикаторов устанавливается m_{ij}. На четвертом этапе рассчитываются ΔP_i и пороги зрелости. На пятом этапе для сочетаний с положительным остаточным эффектом утверждаются меры, сроки и лимиты масштабирования [10; 11; 14; 16; 19].

Оценку следует выполнять до запуска цифрового проекта, после существенного изменения архитектуры и регулярно в ходе эксплуатации. Опережающие индикаторы из матрицы дополняются показателями частоты неуспешных изменений, доступности критических сервисов, среднего времени восстановления, просрочки валидации моделей, концентрации у поставщика, соблюдения целевых сроков восстановления и доли процессов без протестированного ручного или альтернативного режима [3; 10; 11; 16; 19].

Такой подход согласуется с международными наблюдениями. По результатам обследования надзорных практик Базельский комитет относит к частым причинам существенных ИКТ-инцидентов недостатки управления изменениями, проектирования и тестирования систем, управления мощностями и внешними зависимостями [10]. В международных принципах управления операционным риском подчеркиваются роль устойчивости, мониторинга, контроля изменений и сценарного анализа [14; 16]. Для российского финансового рынка аналогичное значение имеют обеспечение технологической независимости, обмен данными об угрозах и повышение киберустойчивости [15].

Предложенный результат развивает вывод M.H. Uddin и соавторов о цифровизации как самостоятельном факторе операционного риска банков [8]. Модель объясняет, почему одно и то же технологическое решение способно приводить к различному результату: воздействие опосредуется масштабом применения и зрелостью контроля. Это согласуется с выводами I. Aldasoro и соавторов о драйверах киберриска [9], M. Hu и соавторов о технологических инновациях и операционном риске [17], M. He, G. Song и Q. Chen о качестве внутреннего контроля [18], а также с исследованиями расходов на кибертехнологии и совокупного банковского риска [20; 21].

Научная новизна исследования состоит в представлении цифровой трансформации как механизма перераспределения операционного риска, а также в разделении валового и остаточного технологического эффекта. Матрица устанавливает связь между технологией, каналом трансформации и измеримым индикатором, а скоринговая модель позволяет определить порог зрелости контроля. Анализ чувствительности дополняет модель проверкой устойчивости решения и позволяет отличить устойчивые оценки от пограничных. В отличие от статического перечня рисков, результат дает основание для решения о допустимости масштабирования конкретного цифрового проекта.

Ограничения исследования связаны с концептуальным характером параметризации, отсутствием эмпирической калибровки коэффициентов и возможным пересечением компонентов риска. Демонстрационные значения не являются оценками конкретной кредитной организации. Для эмпирической верификации необходимы данные о потерях, инцидентах, индикаторах и зрелости контролей в выборке кредитных организаций. Перспективным направлением является оценка параметров a_{ij} и r_{ij} по фактическим данным или результатам формализованного экспертного опроса с проверкой согласованности оценок, а также тестирование нелинейных спецификаций и анализ системного эффекта концентрации облачных, платформенных и модельных решений.

Заключение

Проведенное исследование подтверждает, что воздействие цифровой трансформации на операционный риск кредитных организаций имеет разнонаправленный характер. Автоматизация и аналитика уменьшают часть рутинных ошибок, повышают наблюдаемость процессов и скорость выявления отклонений. Одновременно централизация, масштабирование алгоритмов, внешние зависимости и усложнение цифровой архитектуры повышают потенциальную тяжесть и коррелированность событий.

Основным результатом стала матрица трансформации профиля операционного риска, которая объединяет риск-снижающий эффект, канал усиления и опережающие индикаторы для шести групп технологий. Предложенная скоринговая модель учитывает интенсивность применения технологии, силу разнонаправленных эффектов и зрелость контрольной среды. Выведенный порог зрелости показывает условие, при котором внедрение технологии улучшает соответствующую компоненту профиля. Анализ чувствительности подтвердил устойчивость двух демонстрационных выводов и выявил пограничность третьего, что позволяет использовать устойчивость результата как дополнительный критерий управленческого решения.

Практическое значение подхода заключается в возможности использовать его при предварительной оценке цифровых проектов, установлении требований к контролям, выборе ключевых индикаторов риска и определении допустимого масштаба внедрения. Результаты могут быть встроены в действующую систему управления операционным риском без изменения регуляторной классификации событий.

Для обеспечения устойчивости кредитной организации недостаточно фиксировать рост числа цифровых сервисов. Необходимо контролировать, не сопровождается ли снижение частоты локальных ошибок ростом концентрации, скорости распространения и тяжести редких событий. На уровне банковской сферы такая оценка имеет значение для экономической безопасности, поскольку общие провайдеры, платформы и модели могут формировать коррелированные уязвимости сразу у нескольких участников рынка.

Литература

1. Основные направления развития финансовых технологий на период 2025–2027 годов [Электронный ресурс] / Банк России. – М., 2024. – 65 с. – URL: https://www.cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf (дата обращения: 31.07.2026).
2. Digitalisation of finance [Электронный ресурс] / Basel Committee on Banking Supervision. – Basel: Bank for International Settlements, 2024. – 46 p. – URL: https://www.bis.org/bcbs/publ/d575.pdf (дата обращения: 31.07.2026).
3. Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» [Электронный ресурс]. – URL: https://www.cbr.ru/queries/unidbquery/file/90134/2560 (дата обращения: 31.07.2026).
4. Нафиков Р.Г. Цифровизация банковской системы: риски и возможности управления финансовыми активами // Управленческие науки. – 2022. – Т. 12, № 3. – С. 39–52. – DOI: 10.26794/2304-022X-2022-12-3-39-52.
5. Савчина О.В., Медина Г.В.К. Цифровая трансформация банковского сектора в современных условиях // Вестник МГПУ. Серия: Экономика. – 2023. – № 2 (36). – С. 55–67. – DOI: 10.25688/2312-6647.2023.36.2.05.
6. Лебедева И.А. Цифровая трансформация банковского сектора России: возможности и риски для банков и их клиентов // Социальные новации и социальные науки. – 2022. – № 1. – С. 74–85. – DOI: 10.31249/snsn/2022.01.06.
7. Boot A.W.A., Hoffmann P., Laeven L., Ratnovski L. Fintech: what's old, what's new? // Journal of Financial Stability. – 2021. – Vol. 53. – Art. 100836. – DOI: 10.1016/j.jfs.2020.100836.

8. Uddin M.H., Mollah S., Islam N., Ali M.H. Does digital transformation matter for operational risk exposure? // Technological Forecasting and Social Change. – 2023. – Vol. 197. – Art. 122919. – DOI: 10.1016/j.techfore.2023.122919.
9. Aldasoro I., Gambacorta L., Giudici P., Leach T. The drivers of cyber risk // Journal of Financial Stability. – 2022. – Vol. 60. – Art. 100989. – DOI: 10.1016/j.jfs.2022.100989.
10. Information and communication technology (ICT) risk management: range of practices [Электронный ресурс] / Basel Committee on Banking Supervision. – Basel: Bank for International Settlements, 2026. – 23 p. – URL: https://www.bis.org/bcbs/publ/d611.pdf (дата обращения: 31.07.2026).
11. Principles for the sound management of third-party risk [Электронный ресурс] / Basel Committee on Banking Supervision. – Basel: Bank for International Settlements, 2025. – 22 p. – URL: https://www.bis.org/bcbs/publ/d605.pdf (дата обращения: 31.07.2026).
12. Обзор основных типов компьютерных атак в финансовой сфере в 2025 году [Электронный ресурс] / Банк России, Департамент информационной безопасности. – М.: Банк России, 2026. – 20 с. – URL: https://library.cbr.ru/catalog/lib/books/1043525/ (дата обращения: 31.07.2026).
13. Кодекс этики в сфере разработки и применения искусственного интеллекта на финансовом рынке [Электронный ресурс] / Банк России. – 2025. – URL: https://www.cbr.ru/content/document/file/178667/code_09072025.pdf (дата обращения: 31.07.2026).
14. Revisions to the Principles for the Sound Management of Operational Risk [Электронный ресурс] / Basel Committee on Banking Supervision. – Basel: Bank for International Settlements, 2021. – 23 p. – URL: https://www.bis.org/bcbs/publ/d515.pdf (дата обращения: 31.07.2026).
15. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов [Электронный ресурс] / Банк России. – М., 2023. – 23 с. – URL: https://www.cbr.ru/content/document/file/148351/onrib_2025.pdf (дата обращения: 31.07.2026).
16. Principles for operational resilience [Электронный ресурс] / Basel Committee on Banking Supervision. – Basel: Bank for International Settlements, 2021. – 12 p. – URL: https://www.bis.org/bcbs/publ/d516.pdf (дата обращения: 03.08.2026).
17. Hu M., Zhang Y., Feng X., Xiong X. How technological innovation influence operational risk: Evidence from banks in China // International Review of Financial Analysis. – 2024. – Vol. 95. – Art. 103480. – DOI: 10.1016/j.irfa.2024.103480.
18. He M., Song G., Chen Q. Fintech adoption, internal control quality and bank risk taking: Evidence from Chinese listed banks // Finance Research Letters. – 2023. – Vol. 57. – Art. 104235. – DOI: 10.1016/j.frl.2023.104235.
19. Papathomas A., Konteos G. Financial institutions digital transformation: the stages of the journey and business metrics to follow // Journal of Financial Services Marketing. – 2024. – Vol. 29. – P. 590–606. – DOI: 10.1057/s41264-023-00223-x.
20. Uddin M.H., Mollah S., Ali M.H. Does cyber tech spending matter for bank stability? // International Review of Financial Analysis. – 2020. – Vol. 72. – Art. 101587. – DOI: 10.1016/j.irfa.2020.101587.
21. Chen Z., Li H., Wang T., Wu J. How digital transformation affects bank risk: Evidence from listed Chinese banks // Finance Research Letters. – 2023. – Vol. 58. – Art. 104319. – DOI: 10.1016/j.frl.2023.104319.

Impact of the digital transformation of the banking sector on the operational risk profile of credit institutions

Yakovlev N.A.
Moscow Institute of Economics, Politics and Law (MIEPP)

JEL classification: G20, G24, G28, H25, H30, H60, H72, H81, K22, K34

The study examines how digital transformation reshapes the operational risk profile of credit institutions and develops a comparative assessment tool. The methodology combines comparative and structural-logical analysis, conceptual parametric modelling and one-factor sensitivity analysis. The evidence base includes Bank of Russia and Basel Committee documents for 2021–2026 and relevant Russian and international studies. Digitalisation reduces routine processing errors but can increase concentration, propagation speed and the potential severity of technological, model, cybersecurity and third-party incidents. The paper proposes an operational-risk-profile transformation matrix linking technologies, risk-reducing effects, risk-amplifying channels and leading indicators. A conceptual scoring model separates gross technological effects from residual risk and derives a control-maturity threshold. Varying the risk-amplification and risk-reduction parameters separately by ±20% leaves the qualitative conclusions unchanged for the AI and cloud examples but identifies the open-API case as borderline. The sensitivity check thus distinguishes robust decisions from cases requiring empirical calibration before large-scale deployment. The approach can support ex-ante assessment of digital projects, calibration of key risk indicators, specification of control requirements and periodic updating of operational risk management frameworks.

Keywords: digital transformation, banking sector, credit institution, operational risk, risk profile, artificial intelligence, cloud computing, third-party risk, key risk indicators.

References

1. Bank of Russia. Main directions of financial technology development for 2025–2027. Moscow; 2024. 65 p. Available at: https://www.cbr.ru/Content/Document/File/166399/onfintech_2025-27.pdf (accessed 31 July 2026). (In Russ.).
2. Basel Committee on Banking Supervision. Digitalisation of finance. – Basel: Bank for International Settlements; 2024. – 46 p. Available at: https://www.bis.org/bcbs/publ/d575.pdf (accessed 31 July 2026).
3. Bank of Russia Regulation No. 716-P of 8 April 2020 "On requirements for the operational risk management system in a credit institution and a banking group". Available at: https://www.cbr.ru/queries/unidbquery/file/90134/2560 (accessed 31 July 2026). (In Russ.).
4. Nafikov R.G. Digitalisation of the banking system: risks and opportunities for financial asset management. Upravlencheskie nauki = Management Sciences. 2022;12(3):39–52. – DOI: 10.26794/2304-022X-2022-12-3-39-52. (In Russ.).
5. Savchina O.V., Medina G.V.K. Digital transformation of the banking sector in modern conditions. Vestnik MGPU. Seriya: Ekonomika. 2023;2(36):55–67. – DOI: 10.25688/2312-6647.2023.36.2.05. (In Russ.).
6. Lebedeva I.A. Digital transformation of the Russian banking sector: opportunities and risks for banks and their customers. Sotsial'nye novatsii i sotsial'nye nauki. 2022;(1):74–85. – DOI: 10.31249/snsn/2022.01.06. (In Russ.).
7. Boot A.W.A., Hoffmann P., Laeven L., Ratnovski L. Fintech: what's old, what's new? Journal of Financial Stability. 2021;53:100836. – DOI: 10.1016/j.jfs.2020.100836.
8. Uddin M.H., Mollah S., Islam N., Ali M.H. Does digital transformation matter for operational risk exposure? Technological Forecasting and Social Change. 2023;197:122919. – DOI: 10.1016/j.techfore.2023.122919.
9. Aldasoro I., Gambacorta L., Giudici P., Leach T. The drivers of cyber risk. Journal of Financial Stability. 2022;60:100989. – DOI: 10.1016/j.jfs.2022.100989.
10. Basel Committee on Banking Supervision. Information and communication technology (ICT) risk management: range of practices. – Basel: Bank for International Settlements; 2026. – 23 p. Available at: https://www.bis.org/bcbs/publ/d611.pdf (accessed 31 July 2026).
11. Basel Committee on Banking Supervision. Principles for the sound management of third-party risk. – Basel: Bank for International Settlements; 2025. – 22 p. Available at: https://www.bis.org/bcbs/publ/d605.pdf (accessed 31 July 2026).
12. Bank of Russia, Information Security Department. Review of the main types of computer attacks in the financial sector in 2025. Moscow: Bank of Russia; 2026. 20 p. Available at: https://library.cbr.ru/catalog/lib/books/1043525/ (accessed 31 July 2026). (In Russ.).
13. Bank of Russia. Code of ethics for the development and use of artificial intelligence in the financial market. 2025. Available at: https://www.cbr.ru/content/document/file/178667/code_09072025.pdf (accessed 31 July 2026). (In Russ.).
14. Basel Committee on Banking Supervision. Revisions to the Principles for the Sound Management of Operational Risk. – Basel: Bank for International Settlements; 2021. – 23 p. Available at: https://www.bis.org/bcbs/publ/d515.pdf (accessed 31 July 2026).
15. Bank of Russia. Main directions for the development of information security in the financial sector for 2023–2025. Moscow; 2023. 23 p. Available at: https://www.cbr.ru/content/document/file/148351/onrib_2025.pdf (accessed 31 July 2026). (In Russ.).
16. Basel Committee on Banking Supervision. Principles for operational resilience. – Basel: Bank for International Settlements; 2021. – 12 p. Available at: https://www.bis.org/bcbs/publ/d516.pdf (accessed 3 August 2026).
17. Hu M., Zhang Y., Feng X., Xiong X. How technological innovation influence operational risk: Evidence from banks in China. International Review of Financial Analysis. 2024;95:103480. – DOI: 10.1016/j.irfa.2024.103480.
18. He M., Song G., Chen Q. Fintech adoption, internal control quality and bank risk taking: Evidence from Chinese listed banks. Finance Research Letters. 2023;57:104235. – DOI: 10.1016/j.frl.2023.104235.
19. Papathomas A., Konteos G. Financial institutions digital transformation: the stages of the journey and business metrics to follow. Journal of Financial Services Marketing. 2024;29:590–606. – DOI: 10.1057/s41264-023-00223-x.
20. Uddin M.H., Mollah S., Ali M.H. Does cyber tech spending matter for bank stability? International Review of Financial Analysis. 2020;72:101587. – DOI: 10.1016/j.irfa.2020.101587.
21. Chen Z., Li H., Wang T., Wu J. How digital transformation affects bank risk: Evidence from listed Chinese banks. Finance Research Letters. 2023;58:104319. – DOI: 10.1016/j.frl.2023.104319.